

(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 081 895 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

07.03.2001 Bulletin 2001/10

(51) Int. Cl.7: H04L 12/28, H04L 29/06

(21) Application number: 00103334.9

(22) Date of filing: 21.02.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 03.09.1999 US 389437

(71) Applicant: INTEL CORPORATION
Santa Clara, CA 95052-8119 (US)

(72) Inventors:
• Weatherspoon, Sultan
Vancouver, WA 98682 (US)
• Glendinning, Duncan
Chandler, AZ 85248 (US)

(74) Representative: Botti, Mario
Botti & Ferrari S.r.l.
Via Locatelli, 5
20124 Milano (IT)

(54) Secure wireless local area network

(57) The secure wireless local area network of the present invention includes a single wired network that supports both wired and wireless devices. The network addresses security concerns by including an authentication server that services a plurality of access points. Each access point includes a first authentication device that generates and transmits a first authentication message to the corresponding wireless device over an air channel. The first authentication message includes encrypted validating information about the access point including an access point key that uniquely identifies the access point. Each wireless device includes a second authentication device. The wireless device receives the first authentication message and determines whether the access point is authorized to connect to the wired network. If the access point is valid, the second authentication device responds to the first authentication mes-

sage by generating and transmitting a second authentication message to the access point. The second authentication message includes encrypted validating information about the wireless device and operator, e.g., a device key and the operator's logon name and password. The access point determines the authenticity of the wireless device by decrypting the portion of the second authentication message that includes the device key. If the wireless device is valid, the AP opens a control channel with the authentication server. The AP transmits the first and second authentication messages to the authentication server. If the authentication server validates the access point and the operator's logon name and password, it will authorize access to the wired network.

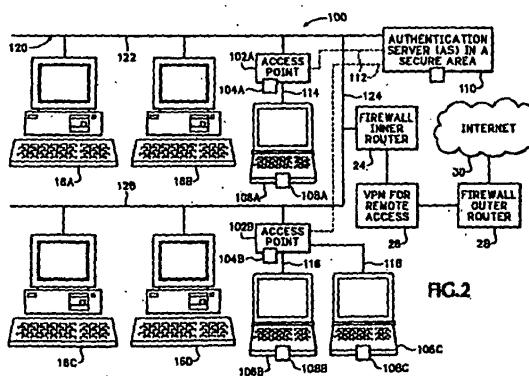


FIG.2

EP 1 081 895 A1

Description**Field of the Invention**

[0001] This invention relates to a wireless local area network and, more particularly, to a secure wireless local area network.

Description of the Prior Art

[0002] A wireless local area network (LAN) is a flexible data communications system implemented as an extension to or as an alternative for a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with operator mobility.

[0003] Wireless LANs have gained strong popularity in a number of vertical markets, including the health-care industry, retail, manufacture, warehousing, and academia. These industries have profited from the productivity gains of using hand-held terminals, personal digital assistants (PDAs), notebook computers, and the like to transmit real-time information to centralized hosts for processing. Today, wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers. With wireless LANs, operators can access shared information without looking for a place to plug in. Wireless LANs offer a variety of productivity, convenience, and cost advantages over traditional wired networks including mobility, installation speed, simplicity, and flexibility, reduced cost of ownership, and scalability. Wireless LANs frequently augment rather than replace wired LAN networks —often providing the final few meters of connectivity between a wired network and the mobile operator.

[0004] Wireless LANs use electromagnetic airwaves (radio or infrared) to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency since the frequency or bit rate of the modulating information adds to the carrier. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies.

[0005] Fig. 1 is a block diagram of a conventional network 10 including a wired LAN 12 and a wireless LAN 14. The wired LAN 12 is often set up as an Intranet. An Intranet is a network designed for information processing within a company or organization. An

Intranet is so called because it usually employs Web pages for information dissemination and applications associated with the Internet, such as Web browsers. It can also include file transfer protocol (FTP) sites, e-mail, and newsgroups and mailing lists accessible only to those within the organization.

[0006] A typical wired LAN 12 includes a plurality of wired devices 16A-D, e.g., desktop personal computers (PCs), connected to the same or different sub-networks (subnets) 18, 20, and 22 terminating at a router (not shown). The wired devices 16A-D are physically connected to each other through cabling (not shown) on the wired LAN 12. For example, PCs 16A and 16B are connected to subnet 18 while PCs 16C and 16D are connected to subnet 20. Subnets 18 and 20 are coupled to each other and to inner firewall router 24 via subnet 22. The inner and outer firewall routers 24 and 28 provide an authorization mechanism that assures only specified operators or applications can gain access to the wired LAN 12. The inner firewall router 24 links the wired LAN 12 to remote users seeking access through the wireless LAN 14 and the Internet 30. The outer firewall 28 limits access to the Virtual Private Network (VPN) server 26 by remote users seeking access through the Internet 30.

[0007] A typical wireless LAN 14 includes at least one access point (AP), the physical cabling (not shown) that connects one AP to another, and at least one wireless device, like devices 34A-C. Common examples of wireless devices 34A-C are hand-held terminals, PDAs, notebook computers, and the like. Other wired and wireless devices are well known to those of skill in the art. An AP, like APs 32A-B, is a transmitter/receiver (transceiver) device that connects to the wireless LAN 14 from a fixed location. At a minimum, the AP receives, buffers, and transmits data between the wireless devices 34A-C and the wireless LAN 14 through an air communications channel. A single AP can support a single wireless device —e.g., AP 32A supports wireless device 34A—or a small group of wireless devices —e.g., AP 32B supports wireless devices 34B and 34C—. The APs can function within a range of less than one hundred to several hundred feet. The AP includes an antenna that is usually mounted high but may be mounted essentially anywhere that is practical so long as the desired radio coverage is obtained.

[0008] The inner firewall router 24 is coupled to the VPN tunnel server 26 and the outer firewall router 28. The VPN server 26 encrypts messages to and from the wired LAN 12 and may provide secondary authentication for remote users. The VPN server 26 uses the Internet 30 to economically connect remote users such as those in branch offices and remote project teams to the wired LAN 12. The VPN server 26 also acts as a gateway between operators of the wireless LAN 14 and the wired LAN 12. The VPN server 26 views access to the wired LAN 12 by the operators of the wireless devices 34A-C the same as remote access by remote users.

Thus, a wireless device operator only has access to other wireless devices on the wireless LAN 14 but does not have automatic access to the Internet 30 or any of the wired devices 16A-D on the wired LAN 12.

[0009] To maximize security and prevent unauthorized access to the wired LAN 12 from a rogue wireless device or AP, the wireless LAN 14 is isolated from the wired LAN 12. Put differently, the cabling that physically connects one wired device to another on the wired LAN 12 is different from the cabling 36 that connects one AP to another on the wireless LAN 14. Isolating the wireless LAN 14 from the wired LAN 12 prevents a wireless device from accessing a wired LAN 12 unless authorized to do so by the VPN server 26 and the inner firewall router 24. However, isolating the wireless LAN 14 from the wired LAN 12 is costly and labor intensive. Moreover, routing the wireless and other remote user traffic through the single VPN server 26 slows access for both, particularly if large files are being transferred. As the VPN server 26 and the firewalls 24 and 28 are busy checking or re-routing data communications packets, they do not flow through the network 10 as efficiently as they would if the VPN server 26 and the firewalls 24 and 28 were not in place. Additionally, if the VPN server 26 fails, wired network 12 access through the VPN server 26 is prevented for both wireless operators and remote users. Another disadvantage to the network 10 is that security is not well integrated. In order for wireless device operators to access the wired LAN 12, the VPN server 26 must authenticate them. This requires the wireless operator to install authentication software (not shown) on the wireless device. The authentication software supported by the VPN server 26 may change or be upgraded requiring the operator to change or upgrade the authentication software installed on his wireless device before the VPN server 26 will authorize access to the wired LAN 12. The high error rate in this type of configuration results in an increased cost of ownership.

[0010] Accordingly, a need remains for a secure wireless local area network that is inexpensive, easy to set up, fast, and reliable.

Summary of the invention

[0011] The secure LAN of the present invention includes a wireless device for use by a wireless device operator. An access point is connected to a wired LAN in communication with the wireless device through an air channel for authenticating the wireless device. An authentication server is connected to the wired LAN for providing the operator with access to the wired LAN after authenticating the access point, the wireless device, and the operator.

Brief description of the drawings

[0012] The foregoing and other objects, features, and advantages of the invention will become more readily apparent from the following detailed description of a preferred embodiment that proceeds with reference to the following drawings.

FIG. 1 is a block diagram of a conventional network;

FIG. 2 is a block diagram of the network of the present invention; and

FIGS. 3A-C is a flow chart of the method for operating a network of the present invention.

Detailed description of the preferred embodiment

[0013] Referring to FIG. 2, the network 100 of the present invention includes a plurality of wired devices 16A-D, e.g., PCs, connected to the same or different sub-networks (subnets) 122, 124, and 126 on the wired LAN 120 terminating at a router (not shown). The wired devices 16A-D are physically connected to each other through the wired LAN 120. The firewall inner and outer routers 24 and 28, respectively, serve the similar function as explained above with reference to FIG. 1. The VPN server 26 limits access to the wired LAN 120 to authorized remote users only.

[0014] A plurality of APs 102A-B is connected directly to the wired LAN 120 at fixed locations. As described earlier with reference to FIG. 1, an AP is a receiver/transmitter (transceiver) device that receives, buffers, and transmits data between a wireless device 106A-C and the wired LAN 120 through a corresponding air communications channel 114, 116, or 118, respectively. Data transmitted over the air channels 114, 116, or 118 is encrypted using a variety of encryption mechanisms including Digital Encryption Standard (DES) endorsed by the National Institute of Standards and Technology, Pretty Good Privacy (PGP), and the like. Encryption mechanisms such as those described above rely on keys or passwords. The longer the key, the more difficult the encryption is to break. The DES standard relies on a 56-bit key length. Some encryption mechanisms have keys that are hundreds of bits long. A single AP can support a single wireless device —e.g., AP 102A supports wireless device 106A—or a small group of wireless devices —e.g., AP 102B supports wireless devices 106B-C.

[0015] To offset security concerns, each AP 102A-B and each wireless device 106A-C includes a corresponding first and second authenticating devices 104A-B and 108A-C, respectively. The authenticating devices 104A-B and 108A-C are preferably tokens installed in the APs 102A-B and wireless devices 106A-C, respectively. Tokens identify a specific user. Smart cards are a type of token. Smart cards resemble the familiar, plain and secure. Each smart card is embedded with an integrated microprocessor and non-volatile memory. Smart cards store information about the holder such as the

holder's personal information —birth date, address, etc.— medical history, or bank account data. Security on smart cards is maintained through a combination of measures including personal identification numbers, passwords, secret keys, and encryption keys stored in the card e.g., session, public, and private encryption keys. An authentication server 110 is connected to the wired LAN 120. The authentication server 110 works in conjunction with the APs 102A-B and the wireless devices 106A-C and their respective authentication devices 104A-B and 108A-C to allow access only to those authorized by the network's administrators.

[0016] The network 100 operates as shown in FIGS. 3A-C. For simplicity, network operation will be described for a single AP 102A supporting a single wireless device 106A. However, a person having skill in the art should recognize that the network 100 can support a plurality of APs and corresponding wireless devices without departing from the principles of the present invention.

[0017] At step 300, the first and second authentication devices 104A and 108A, respectively, are installed in the AP 102A and in the wireless device 106A, respectively. An operator establishes an air communications channel 114 between the wireless device 106A and the AP 102A (step 302). During the establishment of the air channel 114, the AP 102A and the wireless device 106A exchange the encryption mechanism to be used in future communications. At step 304, the first authentication device 104A generates a first authentication message that includes validating information about the AP, e.g., an AP key unique to the AP 102A. The AP key may be a digital signature. A digital signature is a block of data at the end of a message that attests to the authenticity of the file and, consequently, of the AP 102A. If any change is made to the file, the signature will not verify. Thus, digital signatures perform both an authentication and message integrity function.

[0018] The AP encrypts (step 306) and transmits (step 308) the first authentication message to the wireless device 106A. The wireless device 106A receives and decrypts (step 310) the first authentication message and determines whether the AP is a valid access point to the wired LAN 120 (step 312). Authenticating the AP by analyzing the first authentication message ensures that the AP is authorized to be connected to the wired LAN 120 and that it is not a rogue AP set up to facilitate or gain unauthorized access to the wired LAN 120.

[0019] If the AP 102A is not valid, the air communications channel is disabled and communications between the AP 102A and the wireless device 106A terminate (step 314). If the AP 102A is valid, the second authentication device 108A generates (step 316) a second authentication message that, at a minimum, includes a device key identifying the second authentication device 108A as well as the operator's logon name and password. The device key may be known or

unknown to the operator. Validation of the wireless device 106A may involve a challenge response in which the AP 102A requests a certain type of validation from the wireless device 106A, e.g., a digitally signed message. The second authentication device 108A encrypts (step 318) and transmits (step 320) the second authentication message to the AP 102A over the air channel 114. The AP 102A receives the second authentication message and decrypts the portion of the message that includes the device key. At step 322, the AP 102A analyzes the decrypted portion of the second authentication message, i.e., the device key, to determine whether the wireless device 106A is valid.

[0020] If the device key is invalid (step 324), the air communications channel is disabled and communications between the AP 102A and the wireless device 106A terminate (step 314).

[0021] If the device key verifies (step 324), that is, if the wireless device 106A is valid, the AP 102A establishes a control channel 112 with the authentication server 110 at step 326. The AP 102A then transmits (step 328) the encrypted first authentication message and the encrypted portion of the second authentication message that includes the operator's logon name and password to the authentication server 110.

[0022] The authentication server 110 decrypts the first authentication message to verify that the AP 102A is valid (step 330). The authentication server then decrypts the second authentication message to verify the operator's logon name and password (step 330). The authentication server 110 verifies the operator's logon name and password by, e.g., comparing the received logon name and password to a stored list of authorized user names and passwords. If both or either of the AP 102A and the operator are invalid (step 332), the authentication server 110 will deny access to the wired LAN 120 (step 334). If the authentication server 110 validates both the AP and the operator (step 332), the authentication server 110 will enable access to the wired LAN 120 at step 336. The authentication server 110 will enable access to the wired LAN 120 by, e.g., establishing a data channel between the AP and any other device on the wired LAN 120. That is, the authenticated AP and operator will have access to all LAN 120 resources available to wired devices such as devices 16A-D.

[0023] Having illustrated and described the principles of my invention in a preferred embodiment thereof, it should be readily apparent to those skilled in the art that the invention can be modified in arrangement and detail without departing from such principles. I claim all modifications coming within the spirit and scope of the accompanying claims.

55 Claims

1. A secure wireless local area network (LAN), comprising:

7
a wireless device for use by a wireless device operator;

an access point connected to a wired LAN in communication with the wireless device 5 through an air channel for authenticating the wireless device; and

an authentication server connected to the wired LAN for providing the operator with 10 access to the wired LAN after authenticating the access point, the wireless device, and the operator.

2. The secure wireless LAN of claim 1 wherein the 15 access point includes a first authentication device for sending a first authentication message to the wireless device, the first authentication message including validating information about the access point and wherein the wireless device includes a second authentication device for sending a second authentication message to the access point, the second authentication message including validating information about the wireless device and the operator.

3. The secure wireless LAN of claim 2 wherein the 20 access point sends the first and second authentication messages to the authentication server after authenticating the wireless device.

4. The secure wireless LAN of claim 1 comprising:

25 a control channel between the access point and the authentication server for sending an authentication message between the access point and the authentication server, the authentication message including validating information about the access point, wireless device, and operator; and

30 a data channel on the wired LAN for sending data from the wireless device to any other device coupled to the wired LAN, the data channel being enabled after the authentication message is validated by the authentication server.

35 45 50 55 5. A secure wireless local area network (LAN), comprising:

a wireless means for use by a wireless device operator;

an access means connected to a wired LAN for 55 authenticating the wireless means;

an authentication means connected to the

wired LAN for enabling access to the wired LAN after authenticating the access means, the wireless device, and the operator.

6. The secure wireless LAN of claim 5 wherein the access means includes a first authentication means for generating, encrypting, and transmitting a first authentication message to the wireless device, the first authentication message including validating information about the access means and wherein the wireless device includes a second authentication means for generating, encrypting, and transmitting a second authentication message to the access means, the second authentication message including validating information about the wireless device and the operator.

7. The secure wireless LAN of claim 5 comprising:

20 a control channel between the access means and the authentication means for sending an authentication message between the access means and the authentication means, the authentication message including validating information about the access means, the wireless device, and the operator.

8. A method for operating a local area network (LAN), comprising:

25 generating a first authentication message including validating information about an access point connected to a wired LAN;

transmitting the first authentication message from the access point to a wireless device over a wireless channel;

30 validating the access point by analyzing the first authentication message;

generating a second authentication message including validating information about the wireless device and a wireless device operator;

35 transmitting the second authentication message from the wireless device to the access point;

validating the wireless device by analyzing the second authentication message;

40 45 50 55 transmitting the first and second authentication messages to an authentication server after validating the access point and the wireless device;

55 validating the operator; and

enabling a data channel between the wireless device and other devices on the wired LAN after validating the access point and the operator.

5

9. The method of claim 8 wherein transmitting the first authentication message includes transmitting information about the access point contained in a first authentication device and wherein transmitting the second authentication message includes transmitting information about the wireless device and the operator contained in a second authentication device.
10. The method of claim 9 wherein transmitting the first and second authentication messages includes establishing a control channel between the access point and the authentication server.

15

20

25

30

35

40

45

50

55

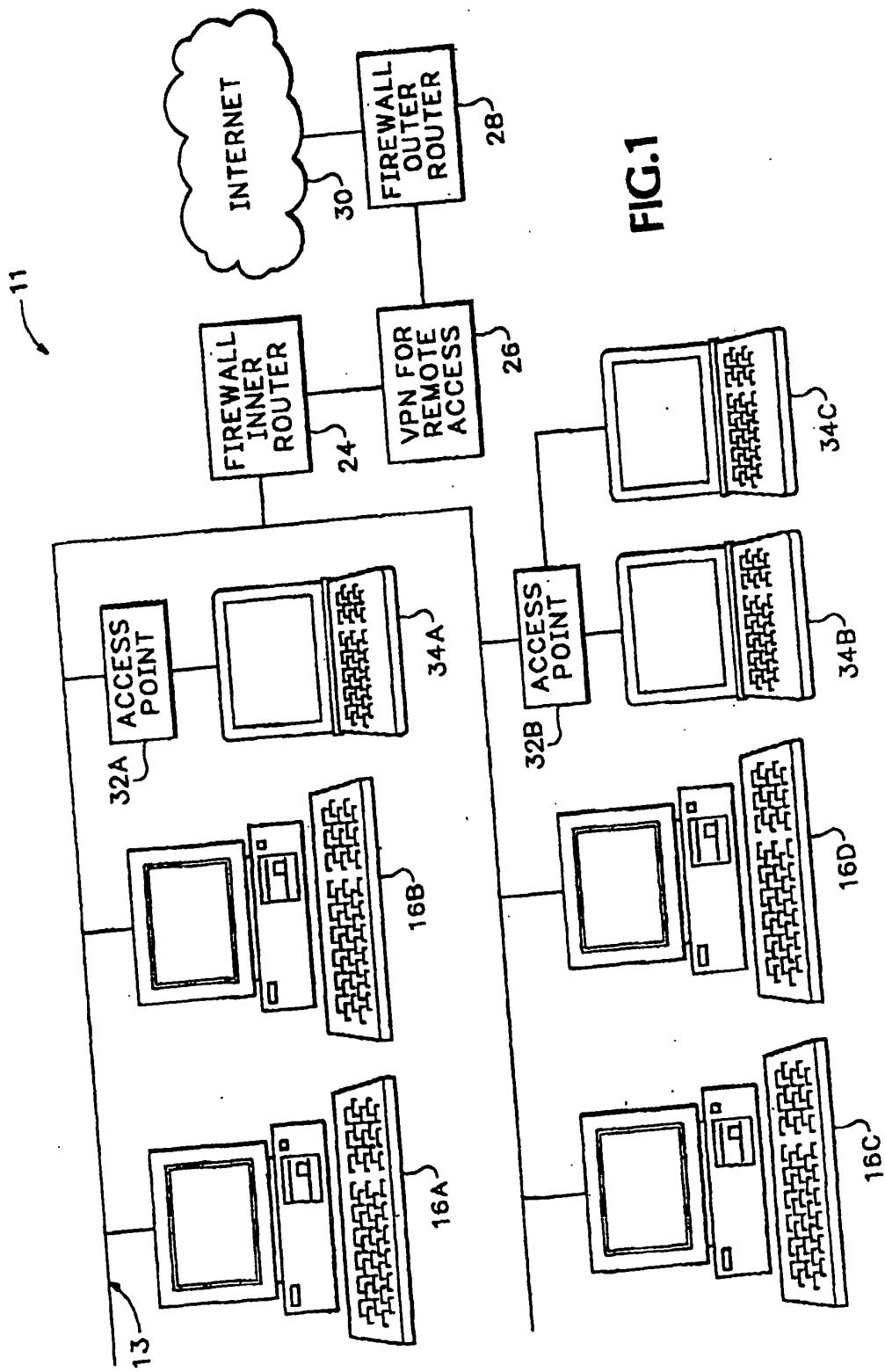
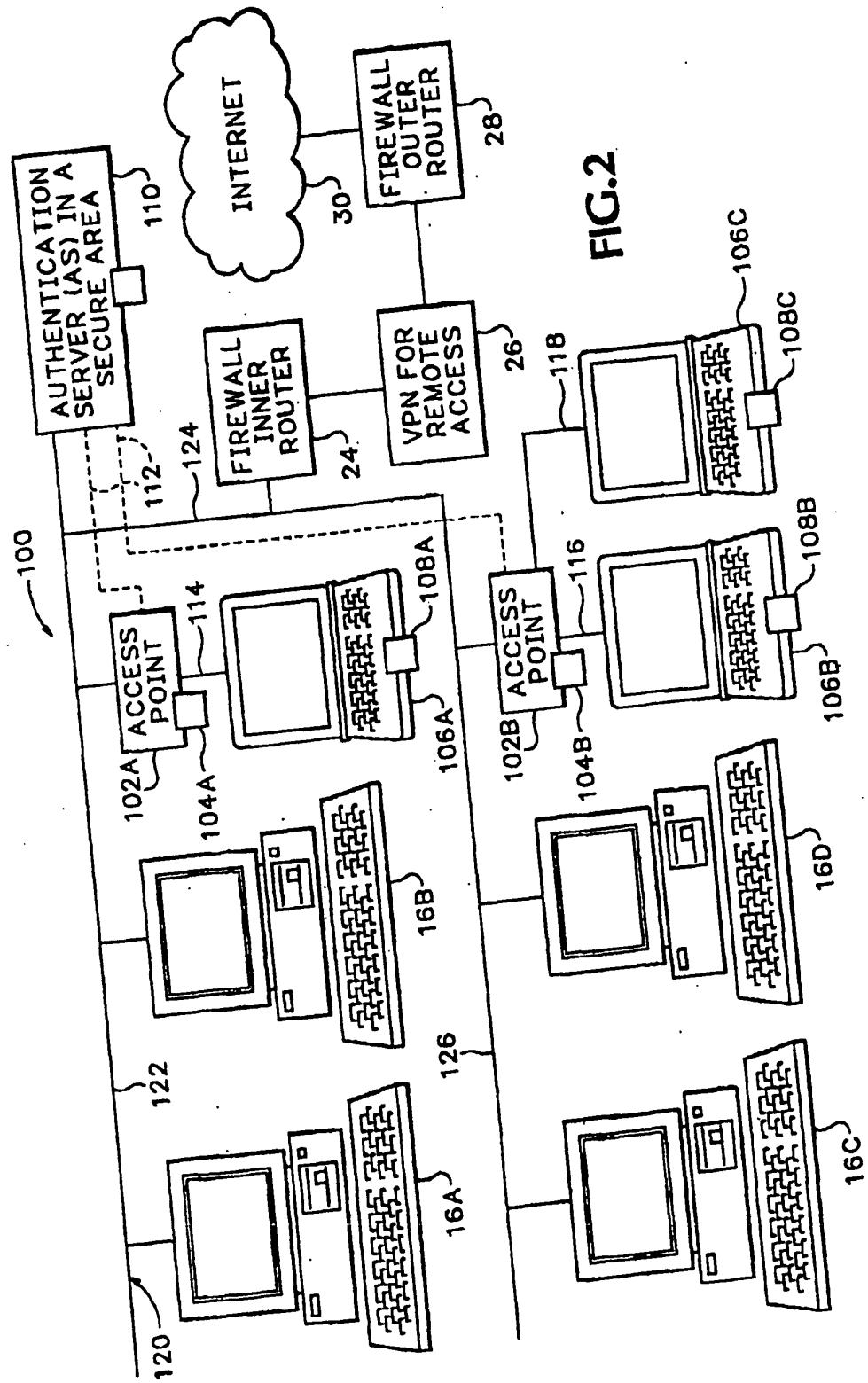


FIG.1



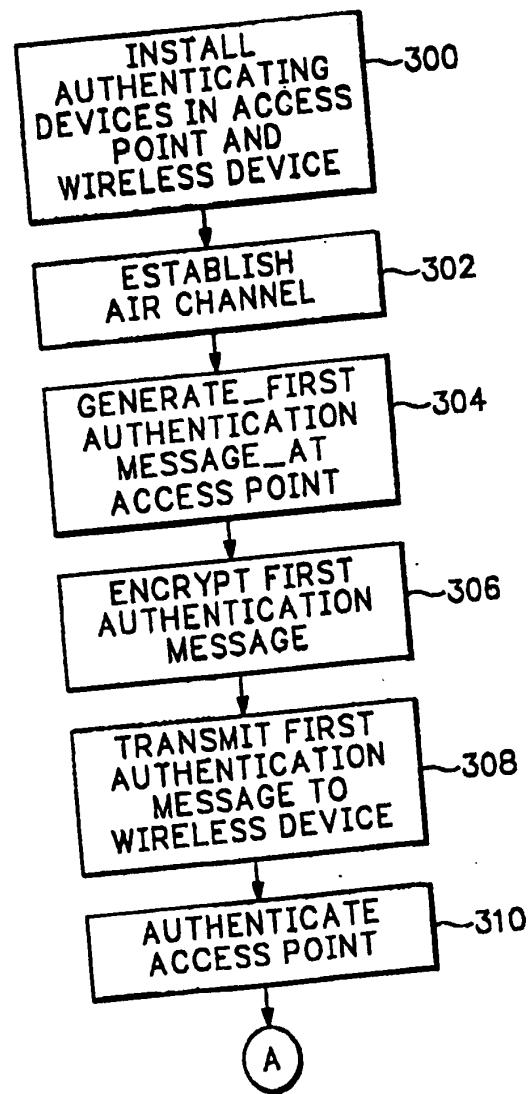


FIG.3A

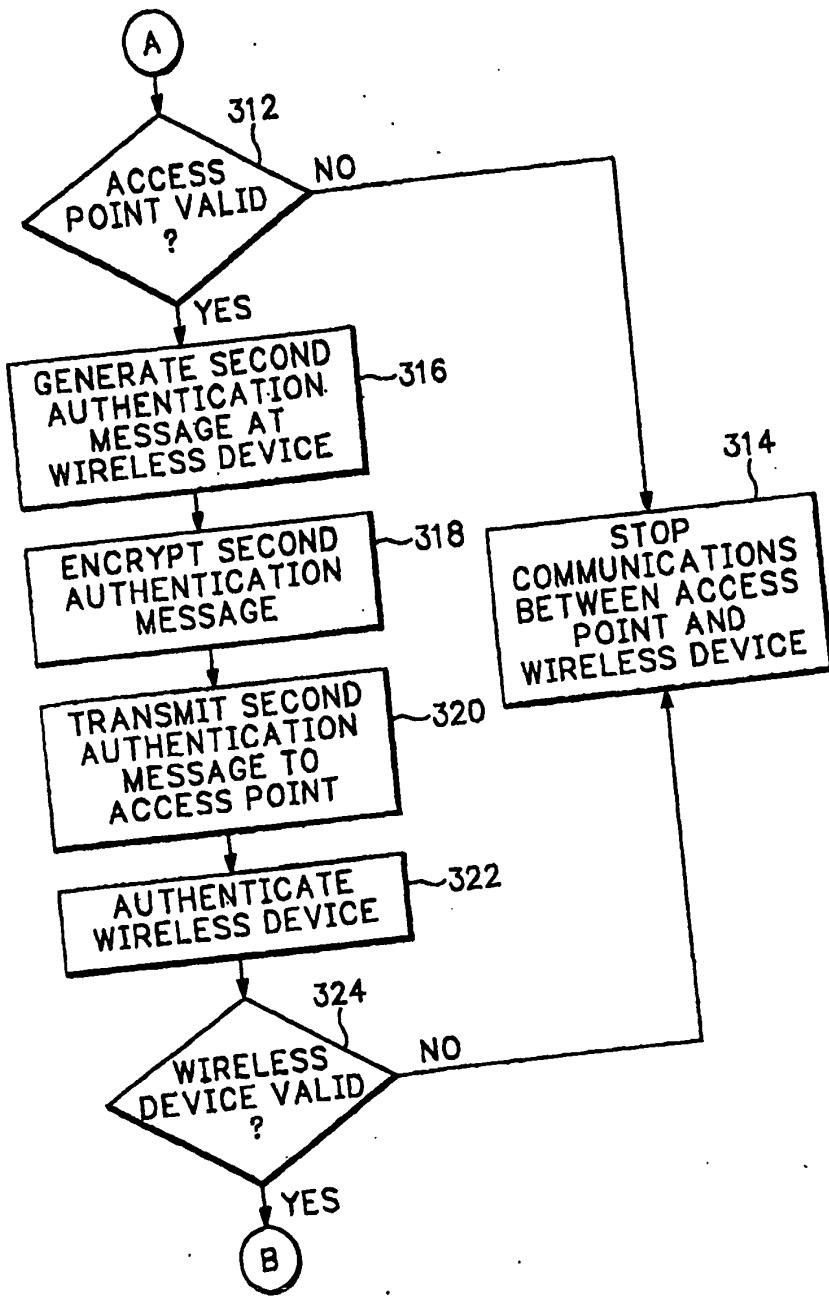


FIG.3B

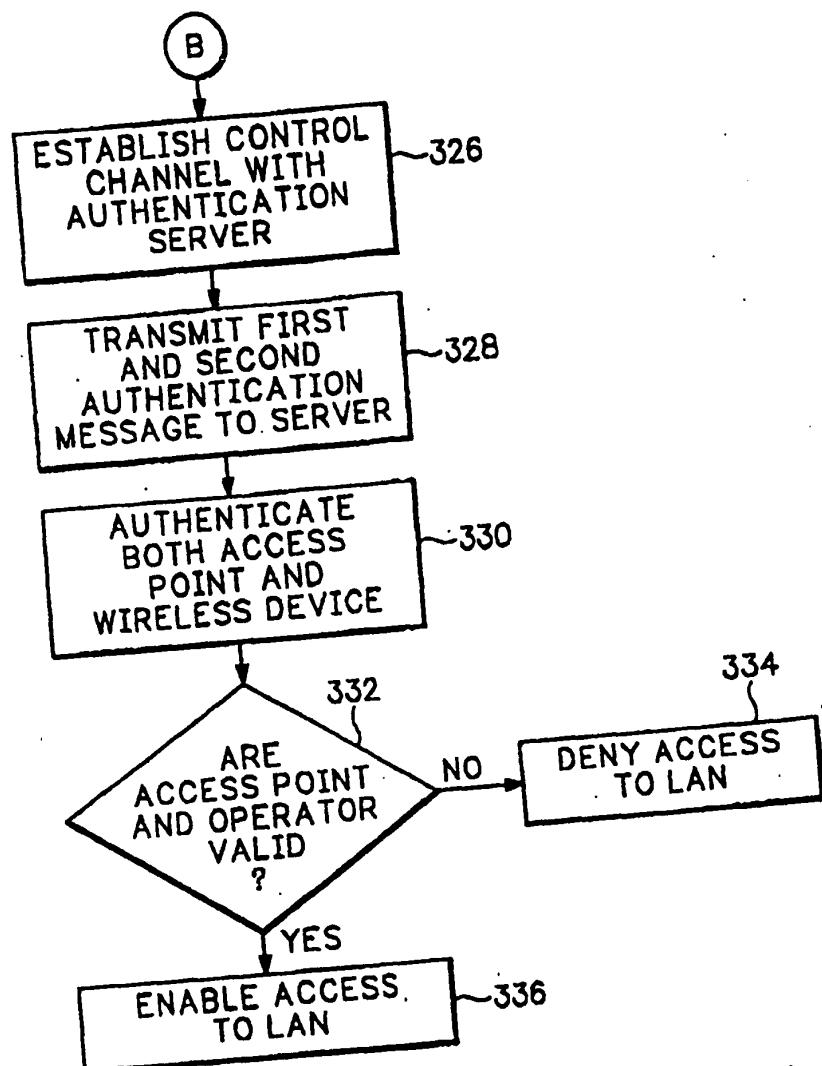


FIG.3C



DOCUMENTS CONSIDERED TO BE RELEVANT					
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.)		
A	WO 99 01969 A (XU YINGCHUN ;3COM CORP (US); CARDWELL BENNETT S (US)) 14 January 1999 (1999-01-14) * page 6, line 2 - page 8, line 22 *	1-10	H04L12/28 H04L29/06		
A	BHARGHAVAN V: "Secure Wireless LANs" PROCEEDINGS OF THE 2ND ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 2 - 4 November 1994, pages 10-17, XP002155490 Fairfax, VA, USA * page 11, right-hand column, line 11 - page 13, left-hand column, line 4 *	1-10			
A	AZIZ A ET AL: "PRIVACY AND AUTHENTICATION FOR WIRELESS LOCAL AREA NETWORKS A SECURE COMMUNICATIONS PROTOCOL TO PREVENT UNAUTHORIZED ACCESS" IEEE PERSONAL COMMUNICATIONS,US,IEEE COMMUNICATIONS SOCIETY, vol. 1, no. 1, 1994, pages 25-31, XP000460718 ISSN: 1070-9916 * page 26, right-hand column, line 43 - page 29, left-hand column, line 24 *	1-10			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">TECHNICAL FIELDS SEARCHED (Int.Cl.)</td> </tr> <tr> <td style="padding: 2px;">H04L</td> </tr> </table>				TECHNICAL FIELDS SEARCHED (Int.Cl.)	H04L
TECHNICAL FIELDS SEARCHED (Int.Cl.)					
H04L					
The present search report has been drawn up for all claims					
Place of search	Date of completion of the search	Examiner			
THE HAGUE	14 December 2000	Weinmiller, J			
CATEGORY OF CITED DOCUMENTS		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons A : technological background O : non-written disclosure P : Intermediate document & : member of the same patent family, corresponding document			
EPO FORM 169 (02.02.2002) (P0201)					

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 00 10 3334

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
 The members are as contained in the European Patent Office EPO file on
 The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-12-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9901969 A	14-01-1999	US 6151628 A	21-11-2000
		AU 8181498 A	25-01-1999
		EP 0927482 A	07-07-1999
		JP 2000503198 T	14-03-2000